Daily Open Source Infrastructure Report
30 November 2012

Top Stories

- A large transformer next to the Westar Energy plant east of Colwich, Kansas, malfunctioned November 28 sparking a fire that burned for several hours. – *Wichita Eagle* (See item **2**)
- SecurityMetrics published its second annual Payment Card Threat Report revealing unencrypted Primary Account Number storage remains alarmingly high, Help Net Security reported November 29. – *Help Net Security* (See item **6**)
- The National Transportation Safety Board recommended improvements and rule changes November 28 after reporting that fire-protection systems on freight aircraft are inadequate. – *CNN* (See item **11**)
- A Santa Barbara, California-based software company, which sued the Chinese government for pirating its flagship content filtering product, has revealed how it was targeted by hackers from that country for the 3 years of the resulting legal proceedings, The Register reported November 29. – *The Register* (See item **41**)

Fast Jump Menu

Energy Sector

1. *November 29, WSAZ 3 Charleston* – (West Virginia) **Break-in causes extensive damage to power sub station.** About 1,500 customers in Charleston, West Virginia lost power November 29. According to an American Electric Power (AEP) spokesperson, someone broke into the company's Chesterfield Avenue station and stole all of the ground wires on its equipment. Power was knocked out in the Kanawha City area near MacCorkle Avenue and the Bridge Road area of South Hills. The spokesperson said the person(s) involved in the incident caused extensive damage to the station and created an extremely dangerous situation so crews had to shut down the station for repairs. Crews were able to switch about 1,500 other customers to alternative sources.
   Source: http://www.wsaz.com/breaking/home/BREAKING-NEWS-Power-Outage-Causing-Traffic-Problems-in-Kanawha-County-181342471.html

2. *November 29, Wichita Eagle* – (Kansas) **Transformer malfunctions at Westar Energy plant near Colwich, causing long-burning fire.** A large transformer next to the Westar Energy plant east of Colwich, Kansas, malfunctioned November 28 sparking a fire that burned for several hours. More than 20 fire trucks were sent to the plant located northwest of Wichita, a Sedgwick County dispatch supervisor said. The fire burned for more than 4 hours. About 12,000 gallons of mineral oil used to cool the transformer caught on fire after a ground wire failed, a Westar spokesman said. Both Westar and Sedgwick County Fire District 1 ruled the fire an accident, but the electric provider's investigation will be ongoing for a few days.
   Source: http://www.kansas.com/2012/11/29/2583115/westar-energy-plant-fire-still.html

For more stories, see items **13** and **46**

[Return to top]

Chemical Industry Sector

3. *November 29, Occupational Health & Safety* – (Ohio) **OSHA Files $545,000 in PSM Penalties after chemical leak.** The Occupational Safety and Health Administration (OSHA) proposed $545,000 in penalties while citing Dover Chemical Co. for 47 health and safety violations, including four alleged willful violations, and has placed the company in its Severe Violator Enforcement Program, which mandates targeted follow-up inspections, Occupational Health & Safety reported November 29. The case began when a breach of a polyvinyl chloride piping system caused a HAZMAT release that temporarily shut down the company's Dover, Ohio plant and an adjacent highway May 21, 2012. All of the willful violations involve process safety management (PSM). Thirty serious violations also relate to PSM, such as inaccurate operating procedures, inadequate information about the hazardous effects of inadvertently mixing different chemicals, not training employees about PSM, and not correcting deficiencies noted during equipment inspections. Eleven of the remaining violations were classified as

serious and two more as other-than-serious. The Dover plant employs about 175 workers and produces chlorinated paraffin, additives for flame-resistant products, and other additives for the plastic, rubber coating, and adhesive and textile product industries. It has been inspected by OSHA four previous times during the past 5 years, according to an OSHA news release.
Source: http://ohsonline.com/articles/2012/11/29/osha-files-545000-in-penalties-after-chemical-leak.aspx?admgarea=news

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *November 28, New Hampshire Public Radio* – (New Hampshire) **Seabrook engineers continue to study deteriorating concrete.** Officials from the Seabrook Nuclear Plant in New Hampshire said the plant is operating safely, despite concrete deterioration found in some structures, New Hampshire Public Radio reported November 28. At the plant's annual press briefing, a communications manager said engineers are studying the deterioration caused by Alkali Silicon Reaction (ASR), a contamination of concrete in structures under water. He pointed out that no such deterioration has been found in critical areas, including the dome housing the plant's radioactive fuel rods. The communications manager said that preliminary studies indicated that that several structures affected by ASR are fully functional, but that the owner, NextEra Energy, will take steps to seal concrete in those areas if the Nuclear Regulatory Commission requires it. NextEra is seeking an extension of its operating license until 2050, and the ASR study will be part of its decision-making process.
Source: http://www.nhpr.org/post/seabrook-engineers-continue-study-deteriorating-concrete

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

5. *November 29, Krebs on Security* – (International) **Online service offers bank robbers for hire.** An online service advertised in the cyber underground lets miscreants hire accomplices in several major U.S. cities to help empty bank accounts, steal tax refunds,

and intercept fraudulent purchases of high-dollar merchandise, Krebs on Security reported November 29. The service, advertised on exclusive, Russian-language forums that cater to cybercrooks, claims to have willing and ready foot soldiers for hire in California, Florida, Illinois, and New York. These associates are not mere "money mules." Rather, as the title of the ad for this service makes clear, the "foreign agents" available through this network are aware that they will be assisting in illegal activity. These complicit "foreign agents" in the U.S. can be hired to launder funds stolen through cyberheists and tax fraud. The proprietors of this service say it will take 40-45 percent of the value of the theft, depending on the amount stolen. In a Q&A with potential buyers, the vendors behind this service say it regularly moves $30,000 – $100,000 per day for clients. Specifically, it specializes in cashing out high-dollar bank accounts belonging to hacked businesses, mentioning fraudulent wire transfers and automated clearinghouse (ACH) payments. According to the advertisement, customers of the service get their own login to a remote panel, where they can interact with the cashout service and monitor the progress of their operations. The service also can be hired to drain bank accounts using counterfeit debit cards obtained through ATM skimmers or hacked point-of-sale devices. The complicit mules will even help cash out refunds from phony State and federal income tax filings.
Source: http://krebsonsecurity.com/2012/11/online-service-offers-bank-robbers-for-hire/

6. *November 29, Help Net Security* – (International) **Unencrypted payment data on business networks at 70 percent.** SecurityMetrics published its second annual Payment Card Threat Report revealing unencrypted Primary Account Number (PAN) storage remains alarmingly high. Virtually no change occurred between 2011 and 2012, with card data storage on corporate systems declining less than one quarter of a percent. The study exposed that greater than 10% of merchants store magnetic stripe track data, essential for the illegal reproduction of credit and debit cards. Financial, hospitality, and retail industries accounted for 55 percent of the total unencrypted payment card data storage among businesses tested. Businesses that store unencrypted payment card data directly violate Payment Card Industry Data Security Standard (PCI DSS) requirements and are more likely to be exploited and suffer severe financial repercussions.
Source: http://www.net-security.org/secworld.php?id=14034&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

7. *November 28, U.S. Federal Bureau of Investigation* – (California) **Glendale con man to plead guilty in fraud scheme that stole $8 million from 30 families.** A Glendale, California man agreed to plead guilty to federal fraud charges, admitting that he ran three separate scams, including a Ponzi scheme that defrauded 30 families out of more than $8 million, according to a November 28 FBI statement. The man also admitted his role in a mortgage fraud scheme that submitted hundreds of falsified loan applications to banks through his brokerage firm, Countywide Financial. He also acknowledged stealing more than $700,000 from his parents by draining their bank accounts and taking out a loan on their home. According to the plea agreement, the man ran an

elaborate Ponzi scheme through his investment company, KGV Investments. He told investors that his contacts gave him unique opportunities to invest in real estate development projects overseas and in the U.S. He convinced more than 30 investors to give him approximately $12 million to invest on their behalf. Instead of investing the money in bond or real estate deals, he used the investors' money for his own benefit.
Source: http://www.loansafe.org/glendale-con-man-to-plead-guilty-in-fraud-scheme-that-stole-8-million-from-30-families

8. *November 28, Reuters* – (California) **SEC charges ex-CEO in Tracinda-linked insider-trading scheme.** The U.S. Securities and Exchange Commission (SEC) November 28 charged the former chief executive of Delta Petroleum Corp with leaking confidential information to a friend about an impending large investment in the company. The SEC said that the former Delta CEO is the central source of an insider-trading scheme that occurred before the Beverly Hills, California-based private investment firm Tracinda Corp had agreed to purchase a 35 percent stake in Delta Petroleum. The SEC's charges against the former CEO come just one month after the agency charged his friend, an insurance executive, for allegedly trading based on the tips he received from the CEO. According to the SEC, the CEO allegedly tipped off the insurance executive and at least one other friend about the upcoming investment by Tracinda. The SEC also claims the CEO told the insurance executive about Delta's confidential third quarter 2007 earnings. All of the various tips helped generate more than $890,000 in illicit profits, the SEC said.
Source: http://www.reuters.com/article/2012/11/28/us-insidertrading-sec-idUSBRE8AR18D20121128

9. *November 28, Reuters* – (California) **Former baseball star indicted for insider trading.** A former Baltimore Orioles third baseman was indicted by a federal grand jury for a $1.3 million insider trading scheme, the U.S. Department of Justice said November 28. He was charged with 42 counts of criminal securities fraud and one count of money laundering over the 2008 purchase of stock in Advanced Medical Optics Inc. based on insider information, according to an indictment filed in a federal court in southern California. The man bought $160,000 worth of stock in Advanced Medical Optics Inc, after a "close personal friend" alerted him to an impending takeover bid by Abbott Laboratories, according to prosecutors. He sold his stock shortly after the takeover bid was announced, making $1.3 million in profits. The criminal charges came on the heels of civil charges filed against him in August 2011 by the U.S. Securities and Exchange Commission (SEC) related to the same accusations. He settled those charges with the SEC, agreeing to pay $2.5 million in fines. The indictment also names three of his friends to whom he provided the insider information.
Source: http://www.reuters.com/article/2012/11/29/us-usa-crime-insidertrading-idUSBRE8AS03820121129

For another story, see item **17**

[Return to top]

Transportation Sector

10. *November 29, Boston Globe* – (Massachusetts) **Six transported to hospital, 20 more evaluated after two trolleys collide at Boylston MBTA station.** Six passengers were injured and 20 others were being evaluated by rescue workers after two Green Line trolleys collided in the Boylston Street Massachusetts Bay Transportation Authority (MBTA) station November 29, the Boston Fire Department said. A witness said the first train was stopped and the doors were open to allow passengers access. An MBTA spokesman said one trolley car "bumped into another," but there was no derailment and no visible damage. He said some passengers were reporting back and neck pain. Rescue workers set up a triage operation on the sidewalk at the station to evaluate the passengers. Six people were taken to the hospital and the rest were being evaluated by the Boston Emergency Medical Services workers, the fire department said. Boylston street westbound between Tremont and Charles streets was closed to traffic.
Source: http://www.boston.com/metrodesk/2012/11/29/trolley-accident-reported-boylston-mbta-station/AFHlk9odLmBbDl87XLRqIO/story.html

11. *November 29, CNN* – (National; International) **Air freight fire protection unsafe, NTSB says.** Fire-protection systems on freight aircraft are inadequate, top U.S. aviation investigators said. The National Transportation Safety Board (NTSB) recommended improvements and rule changes November 28 based on investigations of three catastrophic cargo plane fires. The NTSB chairwoman recommended that the Federal Aviation Administration require better early detection of fires inside cargo containers, development of fire-resistant containers, and requiring active fire-suppression systems on all freight airlines. An NTSB report focused on three cargo fire accidents since 2006. Two of those fires killed the flight crews and destroyed the aircraft. In the third incident, the crew escaped with minor smoke-inhalation difficulties and the plane was significantly damaged. In all three cases, the fires started within the cargo containers aboard the planes, but by the time the plane's fire warning system alerted pilots to the dangers, there was little time for them to react. Federal regulations require cargo airline fire detection systems to alert pilots within a minute of a fire starting, but the NTSB's investigation found current systems detected fire and smoke anywhere from 2 and one-half minutes to more than 18 minutes after the fires start. The NTSB concluded cargo containers made of flammable materials significantly increase the intensity of the on-board fires because there has been little focus by manufacturers or regulators to develop fire-resistant cargo containers. Additionally, the NTSB's report recommended improved fire suppression systems on cargo planes.
Source: http://www.kxly.com/news/Air-freight-fire-protection-unsafe-NTSB-says/-/101270/17583088/-/ygoafv/-/index.html

12. *November 28, ABC News* – (New York) **Boy killed in bedroom when bus crashes into house.** A public bus swerved to avoid a pedestrian and crashed into a house in Hempstead, New York. Nassau County police said the bus veered to avoid hitting the pedestrian then mounted a curb and slammed into a multi-family home, killing a young boy. He was extricated by firefighters and taken to a hospital, where he was pronounced dead an hour later. The pedestrian and 8 of the 11 passengers on the bus were taken to various hospitals with non-life threatening injuries, police said. A

statement from the Nassau Inter County Express bus system said its employees are cooperating with police and have dedicated a team to investigating the crash. The bus was impounded for brake and safety checks and will be inspected by the Public Transportation Safety Board.
Source: http://abcnews.go.com/US/boy-killed-bedroom-bus-crashes-house/story?id=17826688#.ULeAMq6p18E

13. *November 27, Janesville Gazette* – (Wisconsin) **Highway 59 near Milton closed until tomorrow morning.** Highway 59 near Milton, Wisconsin, was closed November 27 and 28 while officials worked to clean up after an accident, according to a news release from the Wisconsin State Patrol. November 27 an ethanol tanker truck tipped over on one of the Highway 59 roundabouts. The accident caused thousands of gallons of ethanol to spill into a nearby retention pond. Officials closed Highway 59 and detoured traffic. According to a news release from the Milton police lieutenant, State and local emergency crews determined it would be safer to let the ethanol continue to spill from the truck than to bring in equipment to stem the spill.
Source: http://gazettextra.com/weblogs/latest-news/2012/nov/27/highway-59-near-milton-closed-until-tomorrow-morni/

[Return to top]

Postal and Shipping Sector

14. *November 29, Jackson County Daily Sentinel* – (Alabama) **Three arrested for mailbox thefts.** Three men allegedly stealing from mail boxes in Jackson County, Alabama, were arrested November 27. A Scottsboro Police official said a witness spotted the suspects going through the mail boxes. There were five victims. The suspects are accused of stealing checks from the mail boxes. "People were mailing bills," police said. "They were going to the boxes and taking the checks for the bills." They were each charged with two counts of theft second degree and three counts of theft third degree.
Source: http://thedailysentinel.com/news/article_6d3c8850-3a37-11e2-9cd2-001a4bcf887a.html

15. *November 28, Creswell Chronicle* – (Oregon) **Man arrested in theft of local mail truck.** A man was arrested November 10 after stealing a Creswell, Oregon post office mail vehicle and having a physical altercation with a Lane County Sheriff's Deputy, the Creswell Chronicle reported November 28. A large amount of stolen mail was recovered from the mail vehicle. According to the Lane County Sheriff's Office, approximately 104 Creswell residents were affected by the mail thefts.
Source: http://www.thecreswellchronicle.com/news/story.cfm?story_no=10852

16. *November 28, WDRB 41 Louisville* – (Kentucky) **Man charged with stealing iPhones at UPS.** A man is behind bars after being charged with stealing 15 iPhones after trying to pass them under security fencing while working at UPS, WDTB 41 Louisville reported November 28. The phones are valued at more than $10,000. Police said he also tried to steal five additional cell phones valued at $3,500 from UPS by wrapping

them in napkins.
Source: http://www.wdrb.com/story/20205830/man-charged-with-stealing-iphones-at-ups

17. *November 28, Associated Press* – (Alabama) **6 arraigned in Ala. identity theft ring.** Six people were arraigned November 28 for their involvement in an identity theft ring. The U.S. Attorney for the Middle District of Alabama said members of the identity theft ring conspired to fraudulently obtain credit cards by diverting mail to a phony mailbox at a Montgomery post office. A postal worker diverted mail, which included credit cards, to the dubious mail box and the suspects ran credit reports on victims before opening accounts in their names. Officials said about $600,000 total was stolen from innocent victims.
Source: http://www.sfgate.com/news/crime/article/6-arraigned-in-Ala-identity-theft-ring-4075330.php

[Return to top]

Agriculture and Food Sector

18. *November 29, Food Safety News* – (International) **CFIA suspends plant after finding Listeria on employee.** After finding Listeria monocytogenes on the sleeve of a meat plant employee, the Canadian Food Inspection Agency (CFIA) suspended the license of a meat processing company in Edmonton, Alberta the week of November 19, saying the company had "failed to correct deficiencies" previously pointed out by the agency. As a result of the positive Listeria test, Capital Packers Inc. recalled certain ham and sausage products that may have been distributed across Canada because the products may be contaminated with the bacteria, though no products have tested positive, according to CFIA, as reported by Food Safety News November 29. The meats subject to the recall were produced November 7, 2012. The agency said that as the food safety investigation progresses, additional products, and additional production dates may be identified, which could lead to a recall expansion.
Source: http://www.foodsafetynews.com/2012/11/cfia-suspends-plant-after-finding-listeria-on-employee/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+foodsafetynews/mRcs+(Food+Safety+News)

19. *November 29, Food Safety News* – (National) **CDC: Salmonella from tahini sickened 23 last year.** Sesame seed paste containing a rare strain of Salmonella sickened 23 people in 7 States and the District of Columbia in 2011, reveals a new report from the U.S. Centers for Disease Control and Prevention (CDC). The article, published in CDC's Morbidity and Mortality Weekly Report the week of November 19, marked the first time the government has told the public about the Salmonella Bovismorbificans outbreak, which lasted from August through November of 2011. Illnesses were largely concentrated in the Mid-Atlantic region, with eight in Washington, D.C., seven in Maryland, three in Virginia, and one apiece in Delaware and New Jersey. Three cases were also reported outside this region – one in California, one in Michigan, and one in New Hampshire.

Source: http://www.foodsafetynews.com/2012/11/government-reports-2011-salmonella-outbreak-linked-to-tahini/

20. *November 29, Associated Press; Middletown Times Herald-Record* – (New York) **2 hurt in boiler blast at upstate NY chicken plant.** Authorities said two people have suffered minor injuries in an explosion at a chicken plant in southeastern New York. The chief of the Fallsburg Fire Department told the Middletown Times Herald-Record that a malfunction at the Murray's Chicken plant filled an industrial boiler with propane. He said the boiler ignited November 28 blowing out a wall of the plant and sending pieces of the boiler flying across the parking lot. Officials said the two people injured in the blast were taken to a local medical center.
Source: http://online.wsj.com/article/AP8ed06682ed284e3bab75a97edbdf9784.html

21. *November 28, WSBT 22 South Bend* – (Indiana) **Fire causes $4M damage at Ind. meatpacking plant.** South Bend, Indiana fire investigators said a cooling system malfunction sparked a blaze at a meatpacking plant, and said damage was more than $4 million. Firefighters were called to Plumrose Meats November 24 when an employee saw smoke coming from the roof. The fire was contained to a mechanical room, causing only $50,000 damage to the building but $4 million damage to contents at the plant. Nearby streets were evacuated as a precaution. The fire could not be investigated at the time of the incident due to a release of ammonia, although the probe was finished November 26.
Source: http://www.firehouse.com/news/10834918/fire-causes-4m-damage-at-ind-meatpacking-plant

22. *November 28, U.S. Food and Drug Administration* – (National) **Sukhi's Gourmet Indian Foods issues voluntary recall of Sukhi's Red Curry Vegetables due to undeclared shrimp.** Sukhi's Gourmet Indian Foods alerted customers November 28 that because of a label error, a single lot code of Red Curry with Vegetables contains undeclared shrimp. Sukhi's voluntarily recalled Lot code 3390113612 with a Use-By Date of May 14, 2013. The product was shipped to distributors in California, Texas, Minnesota, and Georgia, between the dates of May 21, 2012 and October 15, 2012. Sukhi's became aware of the error, after receiving a customer complaint. Investigation into the complaint confirmed that some boxes of a single lot of Red Curry and Vegetables inadvertently contained Yellow Curry with Shrimp.
Source: http://www.fda.gov/Safety/Recalls/ucm329969.htm

[Return to top]

Water Sector

23. *November 29, Northborough Daily Voice* – (Massachusetts) **Marlborough seeks $189,000 from Northborough in sewage fees.** Marlborough, Massachusetts officials said Northborough owes the city a total of $189,000 in payments for sewage treatment for fiscal year 2012 and part of fiscal year 2011, the Northborough Daily Voice reported November 29. Three Northborough properties are connected to Marlborough's sewer system. The sewage is treated at the Westerly Wastewater Treatment Plant in

Marlborough, the Marlborough Commissioner of Public Works said. In a November 27 story in the MetroWest Daily News, the Marlborough mayor was quoted as telling the City Council November 26 that Northborough town officials had not been responsive to requests for payment. Growth in both municipalities requires more sewage capacity, which in turn requires a permit modification from the U.S. Environmental Protection Agency (EPA), the commissioner said. The EPA rescinded its permit in 2010, he added, and has yet to issue a new one. Without a new EPA permit, he said, the city may not have enough capacity to accommodate Northborough's growth. Of the 800,000 gallons per day allocated to the town, he said Northborough's usage had increased recently from 450,000 gallons per day to nearly 550,000 gallons. Marlborough entered into a $30 million contract to expand the Westerly plant and expects Northborough to pay 30 percent of the construction costs, he said.
Source: http://northborough.dailyvoice.com/politics/marlborough-seeks-189000-northborough-sewage-fees

24. *November 29, Pennsylvania Reading Eagle* – (Pennsylvania) **Tilden mobile home park owner faces environmental charges.** A Tilden Township, Pennsylvania mobile home park owner was charged November 28 with illegally discharging untreated sewage into a Schuylkill River tributary and falsifying permit applications, the Pennsylvania Attorney General's office reported. The suspect faces three counts of unlawful conduct under the Clean Air Act and as many counts of tampering with public records, the attorney general said in a prepared release. The attorney general said an investigation revealed that untreated or improperly treated sewage was discharged from the Village at Pleasant Hills Mobile Home Park in Tilden. The park near Hamburg was one of more than 70 that the suspect owns in Pennsylvania, Delaware, and Virginia. For Pleasant Hills and two other mobile home parks in York and Dauphin counties, he also submitted renewal applications for pollutant-discharge permits that contained falsified information regarding sewage treatment, the Attorney General reported. Filed by the attorney general's Environmental Crimes Section, the charges will be prosecuted in Berks County. They come two months after the Pennsylvania Department of Environmental Protection and the U.S. Environmental Protection Agency announced a $1.3 million settlement with the suspect and a series of his corporations, which were accused of violating regulations related to clean drinking water and wastewater treatment.
Source: http://readingeagle.com/article.aspx?id=432013

25. *November 28, Allentown Morning Call* – (Pennsylvania) **Environmental officials probe Vera Cruz sewage leak.** Pennsylvania Department of Environmental Protection (DEP) officials investigated a release of more than 1,000 gallons of sewage along the new Vera Cruz sewer system in Upper Milford Township the week of November 19. The DEP said that the leak on East Main Street in Vera Cruz spewed more than 1,200 gallons onto the street, into a storm sewer, and then into Leibert Creek. Investigators tried to determine the extent of the pollution in Leibert Creek and the Little Lehigh Creek, a primary drinking water source in the area, according to a DEP spokeswoman. She said the rate of the leak was 5 gallons per minute for 4 hours. She said no solids were found in the Leibert Creek, which spills into the Little Lehigh near Emmaus. "Our concern is how much did it affect the Little Lehigh," she said. "It's going to take a few

weeks to determine how much of an impact there was."
Source: http://articles.mcall.com/2012-11-28/news/mc-upper-milford-sewage-leak-20121128_1_sewer-system-public-sewer-service-storm-sewer

26. *November 28, Buffalo News* – (New York) **Residents advised to boil tap water and limit use.** The Chautauqua County, New York Health Department advised residents to boil tap water and limit their water use while repairs were made to the village water plant's treatment system, the Buffalo News reported November 28. The orders were expected to remain in effect until at least December 1. Health officials issued a boil water advisory November 28 after a failure in a chemical feed pump at the plant caused the water to become cloudy. Water plant operators then switched sources to keep additional substandard water from entering the system, drawing from the village's storage tanks and opening a connection to the City of Dunkirk's supply. The volume of water from those sources is limited, however, and residents were urged to cut their water usage in half by limiting showers, shutting off running toilets, and avoiding the use of washing machines and dishwashers. All Fredonia Central School activities November 28 were canceled to save water.
Source:
http://www.buffalonews.com/apps/pbcs.dll/article?AID=/20121128/CITYANDREGION/121129246/1003

27. *November 28, WALA 10 Mobile* – (Alabama) **Sewer problems cause school closings.** The Belforest Water System in Alabama issued a boil water notice for all customers of the system until further notice, WALA 10 Mobile reported November 28. Belforest said the Baldwin County Sewer System accidentally connected a sewer line from a newly constructed residence to a freshwater line. The Belforest water system services Daphne East Elementary School and Daphne Middle School. Both of those schools were closed November 29 due to the issue. Officials said boil water notices are typically issued when monitoring of water being served to consumers contains indicators of contamination or a failure of distribution system integrity evidenced by a loss of system pressure has occurred. Officials said while the notice did not necessary mean the water was contaminated, it does mean that pathogens may have entered the piped-water system. The order was a precautionary notice.
Source: http://www.fox10tv.com/dpp/news/local_news/baldwin_county/belforest-water-system-issues-boil-notice

[Return to top]

Public Health and Healthcare Sector

28. *November 28, KRNV 4 Reno* – (Nevada) **Sierra Plastic Surgery warns patients of possible records breach.** In August of 2012, Reno, Nevada's Sierra Plastic Surgery was informed of a potential data breach of its electronic records, KRNV 4 Reno reported November 28. The data breach occurred between August 11, 2011, – September 23, 2011, by a former employee looking for information on commissions she was owed by getting documents she had previously prepared. The terminated employee may have viewed or printed a copy of patients' surgery estimates, which do

include name and birth date. In rare instances the employee also accessed the name of an insurer, a prescription, surgery notes, a payment balance, and, in less than 50 instances, sensitive payment information including a SSN#, payment information, or personal contact information. The employee's post-employment network access was not fully discovered until August 2012. Sierra Plastic Surgery will soon be notifying affected patients of a potential data breach. Sierra said it has conducted a review of its data storage access and is assured that the data breach will not happen again in the future.
Source: http://www.mynews4.com/news/local/story/Sierra-Plastic-Surgery-warns-patients-of-possible/J4fPQcoRC0muKAhvrvL6pg.cspx

29. *November 28, Senior Housing News* – (National) **Nursing home resident mortality rates skyrocket 218 percent following evacuation.** Senior Housing News reported November 28 that according to a report from the Center for Gerontology and Healthcare Research (CGHR), for nursing home residents suffering from dementia, evacuation from a storm could prove more fatal than the storm itself. Among the three-year study of 21,255 nursing home residents living along the Gulf Coast, the death rate among seniors within 30 days of evacuation jumped 218%. Resident deaths also increased within 90 days after evacuations to 158%. Since the report notes that 50% to 70% of the 1.6 million adults living in nursing homes suffer from a form of dementia, these figures have led to discussions regarding the security of emergency evacuation protocol. CGHR's study notes that the transferring of residents from one location to another could disrupt their continuity of care, therefore leading to a greater risk of hospitalization.
Source: http://seniorhousingnews.com/2012/11/28/nursing-home-resident-mortality-rates-skyrocket-218-following-evacuation/

[Return to top]

Government Facilities Sector

30. *November 29, Associated Press; CBS News* – (International) **Egypt clashes cut off access to U.S. Embassy.** The U.S. Embassy in Cairo, Egypt, closed November 29 after clashes between opposition protesters and riot police cut off access to the building. The clashes have been ongoing as Egypt's Islamist president refuses to back down in a showdown over decrees granting him near-absolute powers. The protesters do not seem to be targeting the embassy itself; they are targeting the riot police. The clashes are happening in the area and in the approaches to and from the embassy. Most embassy staff have gone home, and the embassy closed for all American citizen services.
Source: http://www.cbsnews.com/8301-202_162-57556115/egypt-clashes-cut-off-access-to-u.s-embassy/

31. *November 28, Associated Press* – (South Carolina) **SC Revenue's cyber security job vacant for last year.** The chairman of a Senate panel investigating the exposure of taxpayers' personal data said he is upset to learn that a $25,000 purchase could have prevented the hacking, the Associated Press reported November 28. The chairman also thinks the agency's lack of a computer security officer is partially to blame for the

breach. The Revenue Director told the panel that the position was vacant from September 2011 through August, the month a hacker gained access to the agency's system. The Revenue Director said the former chief information officer could not find anyone willing to accept the job for $100,000. The agency is spending $25,000 on devices that add another security step for someone trying to log into the system remotely. Officials said the devices providing temporary passwords could have prevented the incident.
Source: http://www.wrdw.com/news/headlines/SC-Senate-panel-looking-into-Revenue-hacking-181152801.html

32. *November 28, Associated Press* – (Wisconsin) **Western Wisconsin school hacked for $150K, FBI investigating.** A school district in western Wisconsin said hackers have stolen nearly $150,000 after breaking into its payroll system, the Associated Press reported November 28. The hackers targeted the Stanley-Boyd School District in Chippewa County, according to a report from the La Crosse Tribune. The hackers apparently accessed direct-deposit files from the November 23 payroll, the superintendent said. The district's payroll services are handled by Anchor Bank, which is helping district employees close out their accounts and open new ones in case their account information was compromised, an Anchor Bank spokeswoman said. She said no other Anchor Bank customers were affected. The superintendent said the district is working with bank officials to improve the payroll system's security. The FBI is handling the investigation.
Source: http://www.twincities.com/wisconsin/ci_22080596/western-wisconsin-school-hacked-150k-fbi-investigating

33. *November 28, Inquisitr* – (Pennsylvania) **Pennsylvania science classroom explosion injures eight.** A science classroom explosion and a fire in an eighth grade classroom in Carlisle, Pennsylvania, sent seven students and one teacher to the hospital November 28. Two of the injured children were transported by helicopter from Wilson Middle School to the John Hopkins Hospital in Baltimore for treatment. A Carlisle Regional Medical Center spokeswoman reported that the local facility treated the teacher and five students for minor injuries. The cause of the explosion in the science classroom remains under investigation, according to Fox News. A total of 25 students were in the classroom when the explosion occurred. A Cumberland County Public Safety spokeswoman stated that the fire was quickly contained. The Carlisle Area School District Superintendent told the media that a fireball occurred when some type of chemicals were mixed together. He said the teacher was able to put out the fire with a classroom extinguisher, according to USA Today.
Source: http://www.inquisitr.com/416303/pennsylvania-science-classroom-explosion-injures-eight/

For more stories, see items **1**, **27**, and **45**

[Return to top]

Emergency Services Sector

34. *November 29, Annapolis Capital Gazette* – (Maryland) **Man charged with impersonating police officer.** Anne Arundel County, Maryland police charged a man with impersonating a police officer after he allegedly chased down a cab driver in Glen Burnie November 28. He was charged with four counts of impersonating a police office, reckless endangerment, and first- and second-degree assault, according to online court records. Officers were called to the AA Cab Connection where company representatives reported the incident, a police spokesman said. Employees told officers that the cab driver was traveling on Ritchie Highway when a man claiming to be a police officer began chasing him, apparently over a possible traffic violation. The man followed the cab driver to a parking lot. Employees said the man forced the cab driver to pull over and boxed him in with his vehicle. The man then confronted the cab driver while wearing a jacket with the word "Police" on it. The man then returned to his vehicle and left the scene. Through investigation, police were able to identify the man as the suspect and arrested him at his home.
Source: http://www.capitalgazette.com/news/for_the_record/man-charged-with-impersonating-police-officer/article_136b1c26-3ea3-5a1f-879f-fb9757e9b2c8.html

35. *November 29, Hamden Patch* – (Connecticut) **Police: Woman trashed PD while in custody.** A Hamden, Connecticut woman arrested November 24 after a complaint of loud music at her home allegedly caused thousands of dollars in damage to the booking area of the new Hamden Police Department when she was in custody, according to police. Total damages to the detention area exceeded $5,000, a police spokesman said. She allegedly urinated on the floor, attempted to flood the holding cell, and damaged the sprinkler system. She was charged with two counts of assault on a police officer, interfering with a police officer, first-degree criminal mischief, second-degree criminal mischief, and breach of peace. She was held in lieu of $50,000 bond and is scheduled to appear in court December 7.
Source: http://hamden.patch.com/articles/police-woman-trashed-pd-while-in-custody

36. *November 28, Fayetteville Observer* – (North Carolina) **N.C. teens accused of arson, breaking into station.** Four Fairmont, North Carolina teens, including two junior firefighters, are accused of setting fires to hay bales, woods, a historic building dating to the 1800s, and breaking into a fire department, authorities said. All four were arrested November 27, the lieutenant of the Robeson County Sheriff's Office stated. Two were junior firefighters with the Whitehouse Fire Department for 6 months. The fires were reported in August and November 3, and mostly destroyed hay bales and woods.
Source: http://www.firehouse.com/news/10834884/nc-teens-accused-of-arson-breaking-into-station

37. *November 28, Associated Press* – (Texas) **Pecos man facing federal charges for death threats against police, bomb threats in west Texas.** A west Texas man is in custody on charges he threatened to kill law enforcement officers, members of their families, and detonate bombs, the Associated Press reported November 28. A criminal complaint that led to his arrest by federal agents November 27 outside a Pecos, Texas

truck stop said he used online chat forums to post threats against police in Fort Stockton, Pecos, Big Spring, and Midland. Immigration and Customs Enforcement officials said other threats were made in emails. The threats warned of chemical weapons, car bombs, and high-caliber munitions, Christmas Day carnage and pipe bombs in Pecos, Midland, and Odessa. His detention hearing was scheduled for November 29 in Alpine.
Source: http://www.therepublic.com/view/story/0ccfdc9b4ebc4fe9acb97740e2574586/TX--Police-Death-Threats

38. *November 28, Associated Press* – (Massachusetts) **Nearly 200 released from prison as result of Massachusetts drug lab scandal.** Nearly 200 people have been released from prison and their cases put on hold as a result of a Massachusetts State drug testing lab scandal. The Public Safety secretary told lawmakers at a public hearing November 28 that while investigators are looking at about 34,000 cases overall, 195 individuals have been released, including 79 in Boston. She said their release does not mean they were exonerated. The Health and Human Services secretary said the lack of national accreditation at the lab was one factor that contributed to its troubles. She said the chemist accused of faking lab tests, performed so many more tests than other lab workers should have been a red flag.
Source: http://www.foxnews.com/us/2012/11/28/nearly-200-released-from-prison-as-result-massachusetts-drug-lab-scandal/

39. *November 28, KSL 5 Salt Lake City* – (Utah) **Woman charged with theft for stealing patrol car, leading police on chase.** A woman was charged November 28 with stealing a police vehicle and leading officers on a high-speed chase in St. George, Utah, that ended with her being shot. Investigators said she apparently wanted police to kill her, according to documents filed in 5th District Court. She was charged with aggravated robbery, a first-degree felony, and other charges in connection with the November 19 incident. A St. George police officer arrested her on a warrant and drove her to the jail. When the officer went to open the passenger door for her, he discovered that she had a gun in her hands — which were still handcuffed behind her back. The officer retreated and she was then able to close the doors, move her handcuffs from behind her to the front, make her way to the driver's seat and start the car. A Hurricane police officer saw the police vehicle speeding and initiated a pursuit that eventually continued from Hurricane to Toquerville and on to southbound I-15 until spikes were used to puncture the tires. She was arrested and taken to a nearby medical center.
Source: http://www.ksl.com/?nid=960&sid=23163339

[Return to top]

Information Technology Sector

40. *November 29, The H* – (International) **Google updates all Chrome editions.** Google updated the Stable, Beta, and Developer Channels of the desktop version of its Chrome browser with a number of bug fixes and improvements. The Stable Channel update closes seven security vulnerabilities; three of them rated High, and includes bug fixes.

New stable Chrome versions for iOS and Android were also released and include minor improvements. The iOS version of the browser now supports Apple's Passbook application.
Source: http://www.h-online.com/security/news/item/Google-updates-all-Chrome-editions-1758946.html

41. *November 29, The Register* – (International) **U.S. software firm hacked for years after suing China.** A Californian software company which sued the Chinese government for pirating its flagship content filtering product has revealed how it was targeted by hackers from that country for the 3 years of the resulting legal proceedings. Santa Barbara, California-based Solid Oak Software filed the civil lawsuit against China after discovering thousands of lines of code from its parental filtering CYBERsitter had been lifted and used to develop the Green Dam Youth Escort. Just 12 days after Solid Oak's founder went public with his intentions, the hackers began targeting his employees with a view to infiltrating the company, gleaning intelligence about the court case and disrupting sales as much as possible, Bloomberg reported. The attackers made initial incursions with spyware hidden in malicious email attachments and were soon able to remotely control PCs and switch on webcams to spy on individuals. Solid Oak's Web and email servers were also targeted, frequently crashing several times a day, and the small family-run business dived into the red as customers looking to buy the software online were not able to complete their transactions thanks to some tinkering with the script that controlled payment processing. Forensic investigators said that the malware and attack toolkits they found were unique to Chinese hackers known as the Comment group – a gang fingered for attacks on Coca Cola and others revealed earlier this month. Within two months of a settlement in the case , the attacks reportedly stopped.
Source: http://www.theregister.co.uk/2012/11/29/solid_oak_china_hacked_three_years/

42. *November 28, Dark Reading* – (International) **New hack abuses cloud-based browsers.** Cloud-based browsers that offload processing in the cloud for mobile devices can also be a cybercriminal's best friend: Researchers have found that those browser services can be abused to crack passwords, wage denial-of-service attacks, or perform other unauthorized computations with the free computing power. A team of North Carolina State University and University of Oregon researchers in a proof-of concept used Google's MapReduce technique that allows parallel computing for performing fast computing in the cloud and the Puffin cloud-based browser service. They stored large data packets on URL-shortening sites to disguise the traffic between multiple nodes in order to test how the browsing service could be used for more than browsing. The researchers were able to generate more than 24,000 hashes per second in password-cracking tests with Puffin and their proof-of-concept. With this latest research in what is sometimes called "parasitic computing," the problem lies with the cloud browser providers themselves, whose resources can be abused by bad actors. A North Carolina State researcher said there are ways for cloud-based browsing providers to better monitor their traffic — namely, by associating accounts with the users so they can detect possible abuse or rogue traffic. Cloud browser providers can also limit the computing resources used by each user or client, which also would help detect abuse.
Source: http://www.darkreading.com/cloud-

security/167901092/security/news/240142718/new-hack-abuses-cloud-based-browsers.html

43. *November 28, The Next Web* – (International) **Phishing test: Chrome wins, followed by IE10, Safari, Firefox.** The average phishing URL catch rate in the top four browsers jumped from 46 percent in 2009 to 92 percent in 2012 and the average time it took to block a new phishing URL also improved from 16.43 hours to 4.87 hours, according to a report by NSS Labs. Although all four browsers have improved, some still did better than others: Google Chrome took first place, followed by Microsoft's Internet Explorer (IE) 10, Apple's Safari, and finally Mozilla's Firefox bringing up the rear. The latest results come from a 16-page report titled "Browser Security Comparative Analysis – Phishing Protection", which evaluated the phishing protection offered by the four leading browsers during a 10-day test period. Chrome 21 caught 94 percent of phishing URLs, IE10 stopped 92 percent, Safari thwarted 91 percent, and Firefox denied 90 percent. While the number of reported phishing attacks peaked in 2009, the average number of phishing sites detected has been on the rise from under 40,000 per month in 2011 to over 50,000 per month in 2012. As such, NSS Labs says browsers need to now focus on speeding up blocking response times. The average uptime for sites linked to phishing attacks in 2012 is around 23 hours, down from a high of 73 hours in 2010.
Source: http://thenextweb.com/apps/2012/11/28/latest-phishing-security-test-shows-chrome-is-the-best-followed-by-ie10-safari-and-then-firefox/

44. *November 28, eWeek.com* – (International) **Google Webmaster Tools erroneously reactivates obsolete user accounts.** Google addressed a security hole affecting Google Webmaster Tools that gave users access to obsolete accounts they should not have been able to log into. News of the situation spread across the Web November 28 after reports surfaced about it on search engine optimization (SEO) blogs and news sites. According to Google, for several hours November 27, "a small set" of Webmaster Tools accounts were incorrectly re-verified for people who previously had access. "We've reverted these accounts and are investigating ways to prevent this issue from recurring," a Google spokesperson said.
Source: http://www.eweek.com/cloud/google-webmaster-tools-erroneously-reactivates-obsolete-user-accounts/

45. *November 28, Computerworld UK* – (International) **'Spear phishing' the main email attachment threat.** Some 91 percent of cyber attacks begin with a "spear phishing" email, according to research from security software firm Trend Micro. These attacks may, for instance, refer to their targets by their specific name or job position, instead of using generic titles like in broader phishing campaigns. The goal of a spear phishing attack is to trick the victim into either opening a malicious file attachment or clicking a link to a malware- or an exploit-laden Web site, which could compromise the victim's network. According to the report, 94 percent of targeted emails use malicious file attachments as the payload or infection source. The remaining 6 percent use alternative methods such as installing malware through malicious links. The most commonly used file types for spear phishing attacks accounted for 70 percent of them. The main file types were .RTF (38 percent), .XLS (15 percent), and .ZIP (13 percent). Trend said the

most highly targeted industries for spear phishing were government and activist groups. Information about government agencies and appointed officials are readily found on the internet, said Trend, and often posted on public government Web sites. Because activist groups are highly active in social media, and are also quick to provide member information in order to facilitate communication, organize campaigns, or recruit new members, member profiles are highly visible targets. Trend said 75 percent of email addresses for spear phishing targets are easily found through Web searches or using common email address formats.
Source: http://www.computerworlduk.com/news/security/3413523/spear-phishing-the-main-email-attachment-threat/

For another story, see item **6**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

46. *November 29, Contra Coasta Times* – (California) **Mission Hills mobile home park evacuated due to underground gas leak.** Firefighters helped evacuate some 40 homes at a Mission Hills, California mobile home park November 29 in response to an underground gas leak. The leak occurred at the 193-unit Bermuda Manufactured Home Park, a Los Angeles Fire Department spokesman said. Forty-one firefighters responded and helped around 65 people out of some 40 homes in a "calm and orderly localized evacuation," he said, adding that the evacuees were shuttled to a nearby community clubhouse and no one was endangered by the fumes. A Southern California Gas Company crew arrived at the mobile home park to make repairs. He said the gas was shut and residents began returning to their homes.
Source: http://www.contracostatimes.com/california/ci_22089144/mission-hills-mobile-home-park-evacuated-due-underground

47. *November 28, State Island Advance* – (New York) **Elevated carbon monoxide levels sicken 35 at Staten Island CYO Center.** Dangerously elevated carbon monoxide levels sent 35 victims to the hospital November 27 with complaints of dizziness and nausea at the CYO-MIV Center at Mount Loretto in Pleasant Plains, New York, parents

and emergency officials said. One victim was taken by ambulance to a hospital in Prince's Bay, a hospital spokeswoman said. The remaining victims came in on their own and were treated with oxygen and observed for several hours with repeat blood work. They were all discharged by November 29, though one was transferred to a medical center in Manhattan. Two more were treated November 29. Carbon monoxide readings in the gym were as high as 300 parts per million, according to a city fire department spokesman who said the department considers anything over 10 parts per million a danger. Firefighters evacuated the building and opened access points for ventilation. The source of the elevated levels was a malfunction in one of nine heating units, said a National Grid spokeswoman. She said the utility continued to work with the CYO Center's in-house maintenance staff and heating contractors to find the faulty unit.
Source: http://www.silive.com/southshore/index.ssf/2012/11/elevated_levels_of_carbon_mono.html

48. *November 28, East Central Illinois News-Gazette* – (Illinois) **Police say man was trying to make smoke bomb in apartment.** A suspect who police said tried to make a smoke bomb in his kitchen and sparked a fire was criminally charged. He was charged with felony criminal damage to property and reckless conduct in connection with the fire that happened November 28 in his second-floor apartment in Champaign, Illinois. The fire prompted the evacuation of about 14 residents, who were allowed back into their apartments the same day. A State Attorney said the suspect admitted that he was trying to make a smoke bomb using a recipe and chemicals that he obtained from the Internet. Firefighters were called and arrived to find heavy black smoke when they arrived. Police obtained a search warrant for the apartment and notified the FBI.
Source: http://www.news-gazette.com/news/courts-police-and-fire/2012-11-28/updated-police-say-man-was-trying-make-smoke-bomb-apartment.h

49. *November 28, Bay City News* – (California) **San Francisco: Jewish Community Center evacuated after bomb threat.** A bomb threat called in to the Jewish Community Center of San Francisco November 28 prompted the evacuation of the building in the city's Presidio Heights neighborhood, police and a center spokesman said. The call was received at the front desk of the building, the center spokesman said. The building was evacuated and surrounding sidewalks were closed but no streets were closed, a police sergeant said. The building was deemed safe and the evacuation was lifted about 2 hours later, the center spokesman said.
Source: http://www.marinij.com/ci_22086938/san-francisco-jewish-community-center-evacuated-after-bomb

[Return to top]

National Monuments and Icons Sector

50. *November 28, WSOC 9 Charlotte* – (North Carolina) **Crews continue to battle Caldwell County wildfire.** Crews worked ahead of a wildfire burning in Caldwell County, North Carolina, as they try to keep it from spreading, WSOC 9 Charlotte

reported November 28. The North Carolina Forest Service burned out an area ahead of the main fire, hoping to keep it in check. For 3 days, 50 firefighters have worked to keep the High Eagle fire from spreading. They went on the offensive setting fire to part of the mountainside along a fire line they hoped to hold November 28. Fire investigators were still trying to determine what started the fire located about 8 miles north of Lenoir. They said no homes were threatened at the time, and they want to keep it that way by digging a line around the entire fire. Firefighters expected to be at the scene through November 28. They said by the time they have the fire under control nearly 150 acres will have burned.
Source: http://www.wsoctv.com/news/news/local/crews-continue-battle-caldwell-county-wildfire/nTHmW/

51. *November 28, Gainesville Times* – (Georgia) **Forest service: Wildfire may be contained Thursday.** A 215-acre wildfire near Black and Springer mountains in the Chattahoochee National Forest in Georgia was 85 percent contained November 28, with full containment expected November 29, according to a news release from the U.S. Forest Service. Trail and road closures may be lifted as soon as November 30, the release said. The approach trail to the Appalachian Trail has been closed due to the fire, with the U.S. Forest Service attempting to help through-hikers with shuttles around dangerous portions of the trail. No structures were threatened by the fire that was first reported November 24.
Source: http://www.gainesvilletimes.com/section/6/article/76263/

[Return to top]

Dams Sector

Nothing to report

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2341
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer